Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 – 20. (Canceled)

21. (New) A method for attestation comprising:

performing an attestation scheme using a security module of a user device, said security module being operatively coupled with a verification computer and an attester computer, the performing step comprising steps of:

generating a user attestation-signature value for use with the verification computer, the user attestation-signature value corresponding to at least one attribute, each at least one attribute comprising an attribute value, wherein at least one of the attribute values remain hidden for transactions performable by the user device, the step of generating as performed by the security module comprising the steps of:

providing a module public key and a security module attestation value that is a part of the user attestation-signature value;

receiving from the user device a user public key comprising the user determined attribute value x, y and a proof value demonstrating that the user public key is validly derived from the module public key of the security module;

receiving from the attester computer:

(I) an attestation value comprising the at least one attribute with its corresponding attribute value, wherein at least one of the attribute values are unknown to the attester computer,

the attestation value being derived from an attester secret key, a user public key, and the at least one attester determined attribute values,

the user public key comprising at least one of the user determined attribute

values, and

(II) at least one of the attester determined attribute values (w, z); and

deriving the user attestation-signature value from the attestation value and a security module attestation value,

wherein it is verifiable whether or not

(i) the user attestation-signature value ~~was~~ is validly derived from the security module attestation value and the attestation value, and that

(ii) the attestation value is associated with a subset of at least one attribute, each attribute in the subset comprising a revealed attribute value;

wherein the step of deriving the user attestation-signature value comprises the steps of:

deriving a first security module attestation value;

deriving an intermediate user attestation-signature value from the first security module attestation value under use of an attester public key and a hash function; and

calculating further parts of the user attestation-signature value using at least one of the attribute values, the received part of the user attestation-signature value, the user public key, and the attester public key;

wherein the user public key is derived from the module public key by using the attester public key and the one or more of the attribute values;

wherein the user device provides encryptions under a trusted third party's public key of at least one of the attribute values that remain unknown to the verification computer; and

providing the user attestation-signature value to the verification computer for verification.